Graphical Password Using Captcha for More Secure Authentication Scheme

Parth Patel **Pathan Firdos** **Pantawane Gaurav** **Mr. Sachin N. Wandre**

***Abstract*: A new security primitive for new graphical authentication scheme based on hard artificial intelligence problems. Number of graphical password scheme has been proposed as options to traditional to text password authentication, namely a new family of graphical password system for Captcha technology with the level of security. We propose a new scheme using CAPTCHA (Completely Automated Public Turing Tests to Tell Computers and Humans Apart) that continuing the advantages of graphical password system; Graphical password using Captcha (RPuC) is a both Captcha and graphical password scheme, RPuC covers a number of security problem altogether, such as online guessing attack, relay attack and shoulder-surfing attacks. The level of security maintained and is improved here by the level Captcha we also developed the primitives options for securing the password and for uploading or downloading the data or file from server. Moreover, some primary tries out are conducted and the outcome indicate that the usability should be improved in the future work.**

***Index Terms*— RPuC, graphical password, Captcha, security primitives, password, attack**

I. Introduction

Authentication is indeed at the center of any secure system; a user has to be authenticated before he/she can be affected in online transactions, enter a secured hurdles , open a safe or reach his/her email account. If sensitive information or unauthorized access is given to a wrong identity, the entire security of one system will break down. Generally, the most common and commodious authentication method is the conventional alphanumeric password. However, their built-in security and usability problems led to the development of graphical passwords as choices. A way to tell apart a human from a computer by a test is known as a Turing test. When a computer program is able to generate such tests and calculate the result, it is known as a CAPTCHA. The CAPTCHA is first projected by a study group of Carnegie Mellon University and studied by researchers all over the world after its visual aspects. In the past, Websites have frequently been attacked by malicious programs that register for service monolithic scale.

The system is developed in the domain of security to provide new primitives of authentication so that many different types of attack can be avoided and eliminated. In this project the focus is given on the process of authentication where an user just need an username and password now user need to go through all three levels of security to gain access. We proposed a new security primitive based on hard Artificial Intelligence problems, namely, a new family of graphical password systems built on top of Captcha technology. Server system will generate Captcha for a user and sends back to the user for his authentication purpose. This system can be used for banking application for login, transaction, social networking websites like Gmail, Yahoo, Facebook etc. In military high reached applications, for maintaining important data on servers etc. Under this prototype, the most notable primitive invented is Captcha, which distinguishes human users from computers by presenting a challenge, i.e., a puzzle, beyond the capability of computers but easy for humans. This puzzles are hardest one to crack even a bots cannot break this puzzles. Captcha is now a standard for Internet security technique to protect online email and other services from

Manuscript received Feb, 2013.

Parth J. Patel *Computer Department, University of Pune/ SIT Lonavala. Lonavala, India*
Pathan Firdos J. *Computer Department, University of Pune/ SIT Lonavala. Lonavala, India,*
Gourav R. Pantawane *Computer Department, University of Pune/ SIT Lonavala. Lonavala, India*
Mr. Sachin N. Wandre Assistant Professor *Computer Department, University of Pune/ SIT Lonavala. Lonavala, India,*

being misused or abused by bots. Captcha is now used for reducing the attack on passwords and guessable passwords.

In order to improve the security the password is merge with the Captcha i.e. Captcha is consist of password will term referred as graphical password using Captcha(RPuC). CAPTCHA is now almost a standard for security mechanism for addressing unsuitable or malicious internet bot programs and major web sites such as Google, Yahoo and Microsoft all have their own CAPTCHA for the authentication purpose at the time of sign up.

II. Contribution

Captcha as a graphical password is click based graphical password when sequence of clicks on an image is used to drive the password. Captcha relies on the gap of capabilities between humans and bots in solving certain security problems. This scheme is used to protect the communication channel between user and web server. We are making the improvement in that techniques, which are the levels of authentication is maintained with the three level Captcha. This technique will be most secure and more reliable in terms of secure authentication. In this technique we used many algorithms for Captcha to be reproduced by itself for every new sign up. For Captcha to be reproduce the algorithms are Decentralizes Centralization, scaling, Transformation, DSA (digital signature algorithm) etc. When user wants to upload any type of file he/she has to select the password type (unsecured, secured, more secured).

III. LITERATURE SURVEY

A. EXISTING SYSTEM

The literature survey paper gives an overview about Captcha used as a graphical password for more secure authentication scheme. Recently used techniques for graphical password are not much strong enough and can be breakable by bots easily. Captcha is used to protect sensitive user inputs on a untrusted client. This scheme protects the communication channel between user and Web server from key loggers and spyware, while RPuC is a family of graphical password schemes for user authentication. The paper did not introduce the belief of RPuC or explore its rich properties and the design space of a form of RPuC representation. In the existing systems of graphical password there are more chances of breaking the password because the existing system uses the least secure Captcha with some basic level of security. Captcha is used as 3D animation for authentication but the basic problem is that many browser does not support the animation or they may have basic configuration. It means that the browser should be updated to the latest version.

B. Solution

We introduce a new security primitive based graphical password using Captcha namely a new family of graphical password systems integrating Captcha technology, which we call RPuC. RPuC is click-based graphical passwords, where a sequence of clicks on an image is used to derive a password. Unlike other click-based graphical passwords, images used in RPuC are Captcha challenges, and a new RPuC image is generated for every login attempt.

In this paper we are having three different level of Captcha as level1 Captcha, level2 Captcha, and level3 Captcha. In first level 1 Captcha click based password is needed. The level 1 Captcha includes the characters, numbers; special symbols etc. The character used in the level 1 Captcha can be of different size, different font, and different color. The character can be rotated or scaled and may be contradict with other character. The level 2 Captcha is object based Captcha. This Captcha is having different images as an object user need to click on the object for authentication purpose. In level2 Captcha the series of click is stored for authentication. Every time a user has a new Captcha for log in. The level3 Captcha includes the numeric password where the number is placed at different places in the matrix. The correct chosen of number will have the authorized user and now the user have fully access of files and data from server. This scheme also have an advantage of if the attacker abuse the system after authentication of user then at the time of downloading of file the attacker needs a same password as it mention by the user at the time of sign up. When user wants to upload any type of file he has to select the password type (unsecured, secured, more secured). If he selects any one of them, then according to that captcha will generate. Now if now anyone tries to download the file he has to give the same credential as well. We can use this system in website like Gmail, Facebook, yahoo and in banking transaction.

C. Level1 Captcha (Character Combination)

This level captcha contains the characters, numbers, special symbols etc. the character may be of different font different size and color. The level 1 captcha generates animates this images contains all the information regarding the password. The user needs to click on the proper character to authenticate. There may be possibility that the characters are jumbled with each other. In this situation user need to take care where he/she is going to click. A proper click on character makes user to switch next level captcha. The important note here is that the character can be placed in the image in anywhere in any direction and some time rotated.

D. Level2 Captcha (Objects)

This level has objects in the image. The object are placed at anywhere in the image randomly by the programming algorithm. This object may be small or compact image of any entity of real life. This object are rotated, scaled and set in the image randomly. Here user needs to know the serialization about which object to choose first and all other. The chosen of each object at correct time is matter. The object can be images of animals, rectangle circle etc.

E. Level3 Captcha (Number Grid)

After the above two levels the last level is number grid. This level contains greed of numeric values. This numeric values are not serially arranged but they appear in the greed. The user needs to choose the correct greed for authentication. Each greed has some numeric values and each time of authentication the number place is changed and randomly selected. Here the correct chosen of greed makes user authenticated

IV. RELATED WORK

On the basis of research Captcha is first proposed by a study group of Carnegie Mellon University and studied by researchers all over the world after it comes in existence. The existing system in the past uses the text password only but when Captcha came into picture the text password is merged with Captcha.

The combination of alphabets and number gives a alphanumeric password. This password should be memorable to the user easy and secure. The text password takes as a string for authentication the text password may contains the special symbols like punctuation mark, asterisk etc. Sometimes text passwords are hard to remember and if the password is set simple then the security issues are created.

The next to textual password is graphical password it proves an images with some click point. a user need to click on the image and choose the correct click point in the series to get authenticated. Here only the click points are important with the series of how these points are chosen. In graphical password the click point's values are compared with stored values. Graphical password is easy and reliable to use but it's also have some flaws. After that the graphical password is enhanced by combining it with Captcha.

V.PROPOSED SYSTEM

The project introduce the scheme is a compounding of Captcha and click based graphical password which is less immanent to phishing attacks. Password is created during user registration or after registration and can be changed at the time of registration. A graphical password using Captcha policy is defined by displaying an interface which bears random text Captchas and images. A basic work of security is to create cryptographic primitives based on hard mathematical problems that are computationally intractable. RPuC is click based graphical password when a sequence of clicks on an image, objects and number is used to drive the password. This scheme is used to protect the communication channel between user and web server.

- We are using Captcha for secure authentication in serialize manner. In which we will be handling the issues according to user needs.
- We are maintaining the levels of security with help of levels of Captcha.
- We will handle the issues related to the authentication and keeping data private.
- This project adopts a completely different way to reduce automatic guessing attacks, online attacks.

VI. DISCUSSION AND FUTURE WORK

This projects we have develop the authentication scheme using the Captcha. Captcha is combination of text and images of different size, colors, font etc. this project provides you a three level of Captcha depending on the other Captcha level and the every level has own password to authorize the user. we used many algorithms for our project to generate a different Captcha such as DSA, ,SHA, scaling transformation, centralized decentralization etc.. In future the project can have additional features like a dead zone to overcome from the shoulder surfing attacks. The specific area in the Captcha is permanently known as a dead zone area. This may reduce the shoulder surfing attacks easily. The attacker using shoulder surfing attack can observe the typing position or click points and can easily remember by him/her. Dead zone area may be placed at anywhere in the Captcha but its position will be fix. At time you realize shoulder surfing attack is gone happen the user need to click in the dead zone area which will produce a random Captcha. This Captcha is just to make fool or confuse the attacker. In this Captcha user will do a random clicks on anywhere or at any position. This step of dead zone can be performed by user much time just to improve the security and avoid the shoulder surfing attack.

V. Conclusion

In this paper, we have developed a new authentication scheme for user's password and authorization purpose. Graphical password using Captcha increases the authentication steps to make the user more authenticate. It is a new characteristic of providing security from password as we merge the password and Captcha to make secure and understandable for only authenticated user. This scheme is a great step towards the making the authentication process more secure and reliable for the user. Graphical Password using Captcha has a good potential and refinement which call for useful future work. Also the level of Captcha based password is maintained so to proceed for the next phase first we need to get the proper authentication from previous phase. There are many security primitives but these offers a much secured authentication process. This scheme cab be much more useful where the security and authentication is important such as banking application where user only can access account if it has an proper authentication from all the level of Captcha

REFERENCES

[1] R. Biddle, S. Chiasson, and P. C. van Oorschot, "Graphical passwords: Learning from the first twelve years," ACM Comput. Surveys, vol. 44, no. 4, 2012.

[2] (2012, Feb.). The Science behind Passfaces [Online]. Available:
http://www.realuser.com/published/ScienceBehindPassfaces.pdf

[3] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords," in Proc. 8th USENIX Security Symp., 1999, pp. 1–15.

[4] H. Tao and C. Adams, "Pass-Go: A proposal to improve the usability of graphical passwords," Int. J. Netw. Security, vol. 7, no. 2, pp. 273–292, 2008.

5] J. Bonneau, "The science of guessing: Analyzing an anonymized corpus of 70 million passwords," in Proc. IEEE Symp. Security Privacy, Jun. 2012, pp. 20–25.

[6] S. Kim, X. Cao, H. Zhang, and D. Tan, "Enabling concurrent dual views on common LCD screens," in Proc. ACM Annu. Conf. Human Factors Comput. Syst., 2012, pp. 2175–2184.

[7] S. Li, S. A. H. Shah, M. A. U. Khan, S. A. Khayam, A.-R. Sadeghi, and R. Schmitz, "Breaking e- banking CAPTCHAs," in Proc. ACSAC, 2010, pp. 1–10.

[8] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe, "Purely automated attacks on pass points-style graphical passwords," IEEE Trans. Inf. Forensics Security, vol. 5, no. 3, pp. 393–405, Sep. 2010. Graphical passwords," J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011

[9] P. C. van Oorschot and J. Thorpe, “Exploiting predictability in click based graphical passwords,” J. Comput. Security, vol. 19, no. 4, pp. 669–702, 2011.

[10] R. Lin, S.-Y. Huang, G. B. Bell, and Y.-K. Lee, “A new CAPTCHA interface design for mobile devices,” in Proc. 12th Austral. User Inter. Conf., 2011, pp. 3–8.

Parth J. Patel *B.E Computer Department, University of Pune/ SIT Lonavala, Lonavala, India,*

Pathan Firdos J. *B.E. Computer Department, University of Pune/ SIT Lonavala,). Lonavala, India,*

Gourav R. Pantawane *B.E Computer Department, University of Pune/ SIT Lonavala. Lonavala, India,*